CLAIMS

What is claimed is:

1. A method for detecting an attack on a data processing system, the method comprising, in the data processing system:

providing an initial secret;

binding the initial secret to data indicative of an initial state of the system via a cryptographic function;

recording state changing administrative actions performed on the system in a log;

prior to performing each state changing administrative action, generating a new secret by performing the cryptographic function on a combination of data indicative of the administrative action and the previous secret, and erasing the previous secret;

evolving the initial secret based on the log to produce an evolved secret;

comparing the evolved secret with the new secret;

determining that the system is uncorrupted if the comparison indicates a match between the evolved secret and the new secret; and

determining that the system in corrupted if the comparison indicates a mismatch between the evolved secret and the new secret.

2. A method as claimed in claim 1, wherein the cryptographic function comprises a one-way hash function.

3. A method as claimed in claim 2, wherein the hash function comprises an exponentiation function.

4. A method as claimed in claim 1, wherein the cryptographic function comprises a public/private key pair.

5. A method as claimed in claim 1, comprising receiving the initial secret from a system administrator.

6. A data processing system comprising:

a processor;

a memory connected to the processor; and

detection logic connected to the processor and the memory, the detection logic, in use:

providing an initial secret;

binding the initial secret to data indicative of an initial state of the system via a cryptographic function;

recording state changing administrative actions performed on the system in a log;

prior to performing each state changing administrative action, generating a new secret by performing the cryptographic function on a combination of data indicative of the administrative action and the previous secret, and erasing the previous secret;

evolving the initial secret based on the log to produce an evolved secret;

comparing the evolved secret with the new secret;

determining that the system is uncorrupted if the comparison indicates a match between the evolved secret and the new secret; and

determining that the system in corrupted if the comparison indicate a mismatch between the evolved secret and the new secret.

7. A system as claimed in claim 6, wherein the cryptographic function comprises a one-way hash function.

8. A system as claimed in claim 7, wherein the hash function comprises an exponentiation function.

9. A system as claimed in claim 6, wherein the cryptographic function comprises a public/private key pair.

10. A system as claimed in claim 6, wherein the detector logic receives the initial secret from a system administrator.

11. A computer program element comprising computer program code means which, when loaded in a processor of a computer system, configures the processor to perform a method as claimed in claim 1.

12. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing detection of an attack on a data processing system, the computer readable program code means in said article of manufacture comprising computer readable

program code means for causing a computer to effect the steps of claim 1.

13. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for detecting an attack on a data processing system, said method steps comprising the steps of claim 1.

14. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing a data processing system, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 6.

15. A method for cryptographic entangling of state and administration in a data processing system, the method comprising:

initializing the system by generating an initial secret

releasing binding data;

binding the binding data to the initial secret;

updating the initial secret in advance of an administrative action by computing a new secret;

erasing the initial secret together with any information from which the initial secret might be derived;

recording data indicative of the administrative action;

permitting execution of the administrative action;

offering a proof that the new secret corresponds to the initial secret as it has evolved according to a record of administrative actions.

16. A method as recited in claim 15, wherein the step of offering retrieves the initial secret via a request for entry of the initial secret by a system administrator, retrieving the record of administrative actions previous stored; and

evolving a candidate secret for the initial secret based on the record of administrative actions retrieved;

comparing the candidate secret with a current secret;

if the candidate secret matches the current secret, reporting that the data processing system is still in an uncorrupted state, and

if the candidate secret does not match the current secret, reporting that the data processing system is in a potentially compromised state.

17. A method as recited in claim 15, further comprising permitting detection of any Trojan horse within the system.

18. A method as recited in claim 15, wherein the initial secret is supplied via a secure communication channel.

19. A method as recited in claim 15, wherein the binding data takes different forms depending on the data processing system, an application of the data processing system, and a trust mechanisms associated with communication of the initial secret.

20. A method as recited in claim 15, wherein the administrative action is an action taken from a group of actions consisting of: updating of system executable code; updating of system libraries; installation of kernel modules; reading of files such as those used to store system states during rebooting operations; alteration of configuration files; alteration of system run-level codes; writing to or reading from peripheral devices; and any combination of these actions.

20. A method as recited in claim 15, wherein the step of computing the new secret includes applying a one way function to a combination of a previous secret and data indicative of the administrative action.

21. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing cryptographic entanglement of state and administration in a data processing system, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 15.

22. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for cryptographic entangling of state and administration in a data processing system, said method steps comprising the steps of claim 15.